

## **AMENDMENTS TO THE CLAIMS**

This listing of claims will replace all prior versions, and listings, of claims in the application:

### **Listing of Claims:**

1. (Currently amended) A method for operating a key distribution center (KDC) that provides keys to facilitate secure communications between clients and servers across a computer network, wherein the KDC operates without having to store long-term server secrets, comprising:
  - 5 receiving a communication from a server that is authenticated at the KDC;
  - 6 wherein the communication includes a temporary secret key to be used in
  - 7 communications with the server for a limited time period, and wherein the
  - 8 temporary secret key is shared between the server and the KDC; and
  - 9 storing the temporary secret key in a database at the KDC, so that the
  - 10 temporary secret key can be subsequently used to facilitate one or more
  - 11 communications between a client and the server, ~~wherein the temporary secret key is encrypted with a public key belonging to the KDC, so that the temporary secret key can only be decrypted using a private key belonging to the KDC;~~
  - 12 wherein the temporary secret key is a short-term secret which becomes
  - 13 invalid after a short time period; and wherein ~~the server generates a new temporary secret key a new temporary secret key is generated~~ in response to a
  - 14 request from the KDC for a new temporary secret key to replace the invalid
  - 15 temporary secret key, thereby avoiding the overhead of periodically establishing a
  - 16 new temporary secret key.

1           2. (Original) The method of claim 1, wherein upon subsequently receiving  
2 a request from the client at the KDC to communicate with the server, the method  
3 further comprises facilitating communications between the client and the server  
4 by:

5           producing a session key to be used in communications between the client  
6 and server;

7           creating a ticket to the server by encrypting an identifier for the client and  
8 the session key with the temporary secret key for the server; and

9           assembling a message that includes the identifier for the server, the session  
10 key and the ticket to the server; and

11           sending the message to the client in a secure manner; and

12           allowing the client to forward the ticket to the server in order to initiate  
13 communications between the client and the server.

1           3. (Original) The method of claim 2, wherein upon receiving the ticket  
2 from the client at the server, the method further comprises:

3           decrypting the ticket at the server using the temporary secret key to restore  
4 the session key and the identifier for the client; and

5           using the session key at the server to protect subsequent communications  
6 between the server and the client.

1           4. (Original) The method of claim 2, wherein assembling the message  
2 involves including an expiration time for the session key in the message.

1           5. (Original) The method of claim 2, wherein allowing the client to  
2 forward the ticket to the server includes allowing the client to forward an  
3 identifier for the temporary secret key to the server, so that the server can know  
4 which temporary secret key to use in decrypting the ticket.

1           6. (Original) The method of claim 2, wherein sending the message to the  
2 client in the secure manner involves encrypting the message with a second session  
3 key that was previously communicated to the client by the KDC.

1           7. (Original) The method of claim 2, further comprising alternatively  
2 creating the ticket to the server by encrypting the identifier for the client and the  
3 session key with one of:  
4           a public key for the server; and  
5           a secret key for the server previously agreed upon between the server and  
6 the KDC and stored at the KDC.

1           8. (Original) The method of claim 1, wherein receiving the communication  
2 from the server involves authenticating the server.

1           9. (Original) The method of claim 8, wherein authenticating the server  
2 involves using authentication information pertaining to the server, the  
3 authentication information including a certificate chain from a trust anchor to the  
4 server, and including a server public key that is associated with a server private  
5 key to form a public key-private key pair associated with the server.

1           10. (Original) The method of claim 8, wherein authenticating the server  
2 involves authenticating the server without having prior configuration information  
3 pertaining to the server at the KDC.

1           11. (Original) The method of claim 8, wherein authenticating the server  
2 includes using a server public key that is stored locally in the KDC.

1           12 (Canceled).

1           13. (Original) The method of claim 1, wherein the communication is  
2 signed with a server private key so that the KDC can use a corresponding server  
3 public key to verify that the communication was sent by the server.

1           14. (Original) The method of claim 1, wherein the communication is  
2 received in response to a request being sent by the KDC to the server indicating  
3 that the temporary secret key is needed from the server.

1           15. (Original) The method of claim 1, further comprising communicating  
2 information to the server that enables the server to authenticate the KDC.

1           16. (Original) The method of claim 1, wherein the KDC operates in  
2 accordance with the Kerberos standard.

1           17. (Original) The method of claim 1, wherein the communication  
2 received from the server additionally includes an identifier for the server.

1           18. (Original) The method of claim 1, further comprising propagating the  
2 temporary secret key to multiple KDCs.

1           19. (Currently amended) A computer-readable storage medium storing  
2 instructions that when executed by a computer cause the computer to perform a  
3 method for operating a key distribution center (KDC) that provides keys to  
4 facilitate secure communications between clients and servers across a computer  
5 network, wherein the KDC operates without having to store long-term server  
6 secrets, the method comprising:  
7           receiving a communication from a server that is authenticated at the KDC;

8       wherein the communication includes a temporary secret key to be used in  
9   communications with the server for a limited time period, and wherein the  
10   temporary secret key is shared between the server and the KDC; and  
11           storing the temporary secret key in a database at the KDC, so that the  
12   temporary secret key can be subsequently used to facilitate one or more  
13   communications between a client and the server; ~~wherein the temporary secret key~~  
14   ~~is encrypted with a public key belonging to the KDC, so that the temporary secret~~  
15   ~~key can only be decrypted using a private key belonging to the KDC;~~  
16           wherein the temporary secret key is a short-term secret which becomes  
17   invalid after a short time period; and wherein the server generates a new  
18   temporary secret key ~~a new temporary secret key is generated~~ in response to a  
19   request from the KDC for a new temporary secret key to replace the invalid  
20   temporary secret key, thereby avoiding the overhead of periodically establishing a  
21   new temporary secret key.

1       20. (Original) The computer-readable storage medium of claim 19,  
2   wherein upon subsequently receiving a request from the client at the KDC to  
3   communicate with the server, the method further comprises facilitating  
4   communications between the client and the server by:  
5           producing a session key to be used in communications between the client  
6   and server;  
7           creating a ticket to the server by encrypting an identifier for the client and  
8   the session key with the temporary secret key for the server; and  
9           assembling a message that includes the identifier for the server, the session  
10   key and the ticket to the server; and  
11           sending the message to the client in a secure manner; and  
12           allowing the client to forward the ticket to the server in order to initiate  
13   communications between the client and the server.

1           21. (Original) The computer-readable storage medium of claim 20,  
2   wherein upon receiving the ticket from the client at the server, the method further  
3   comprises:

4           decrypting the ticket at the server using the temporary secret key to restore  
5   the session key and the identifier for the client; and  
6           using the session key at the server to protect subsequent communications  
7   between the server and the client.

1           22. (Original) The computer-readable storage medium of claim 20,  
2   wherein assembling the message involves including an expiration time for the  
3   session key in the message.

1           23. (Original) The computer-readable storage medium of claim 20,  
2   wherein allowing the client to forward the ticket to the server includes allowing  
3   the client to forward an identifier for the temporary secret key to the server, so that  
4   the server can know which temporary secret key to use in decrypting the ticket.

1           24. (Original) The computer-readable storage medium of claim 20,  
2   wherein sending the message to the client in the secure manner involves  
3   encrypting the message with a second session key that was previously  
4   communicated to the client by the KDC.

1           25. (Original) The computer-readable storage medium of claim 20,  
2   wherein the method further comprises alternatively creating the ticket to the server  
3   by encrypting the identifier for the client and the session key with one of:  
4           a public key for the server; and  
5           a secret key for the server previously agreed upon between the server and  
6   the KDC and stored at the KDC.

1           26. (Original) The computer-readable storage medium of claim 19,  
2   wherein receiving the communication from the server involves authenticating the  
3   server.

1           27. (Original) The computer-readable storage medium of claim 26,  
2   wherein authenticating the server involves using authentication information  
3   pertaining to the server, the authentication information including a certificate  
4   chain from a trust anchor to the server, and including a server public key that is  
5   associated with a server private key to form a public key-private key pair  
6   associated with the server.

1           28. (Original) The computer-readable storage medium of claim 26,  
2   wherein authenticating the server involves authenticating the server without  
3   having prior configuration information pertaining to the server at the KDC.

1           29. (Original) The computer-readable storage medium of claim 26,  
2   wherein authenticating the server includes using a server public key that is stored  
3   locally in the KDC.

1           30 (Canceled).

1           31. (Original) The computer-readable storage medium of claim 19,  
2   wherein the communication is signed with a server private key so that the KDC  
3   can use a corresponding server public key to verify that the communication was  
4   sent by the server.

1           32. (Original) The computer-readable storage medium of claim 19,  
2   wherein the communication is received in response to a request being sent by the

3 KDC to the server indicating that the temporary secret key is needed from the  
4 server.

1 33. (Original) The computer-readable storage medium of claim 19,  
2 wherein the method further comprises communicating information to the server  
3 that enables the server to authenticate the KDC.

1 34. (Original) The computer-readable storage medium of claim 19,  
2 wherein the KDC operates in accordance with the Kerberos standard.

1 35. (Original) The computer-readable storage medium of claim 19,  
2 wherein the communication received from the server additionally includes an  
3 identifier for the server.

1 36. (Original) The computer-readable storage medium of claim 19,  
2 wherein the method further comprises propagating the temporary secret key to  
3 multiple KDCs.

1 37. (Currently amended) An apparatus that provides keys to facilitate  
2 secure communications between clients and servers across a computer network,  
3 wherein the apparatus operates without having to store long-term server secrets,  
4 comprising:

5 a key distribution center (KDC);  
6 a receiving mechanism within the KDC that is configured to receive a  
7 communication from a server;

8 wherein the communication includes a temporary secret key to be used in  
9 communications with the server for a limited time period, and wherein the  
10 temporary secret key is shared between the server and the KDC; and

11           a storage mechanism within the KDC that is configured to store the  
12 temporary secret key in a database at the KDC, so that the temporary secret key  
13 can be subsequently used to facilitate one or more communications between a  
14 client and the server; ~~wherein the temporary secret key is encrypted with a public  
15 key belonging to the KDC, so that the temporary secret key can only be decrypted  
16 using a private key belonging to the KDC;~~  
17           wherein the temporary secret key is a short-term secret which becomes

18 invalid after a short time period; and wherein ~~the server generates a new  
19 temporary secret key a new temporary secret key is generated in response to a  
20 request from the KDC for a new temporary secret key to replace the invalid  
21 temporary secret key, thereby avoiding the overhead of periodically establishing a  
22 new temporary secret key.~~

1           38. (Original) The apparatus of claim 37, further comprising a  
2 communication facilitation mechanism within the KDC, wherein upon receiving a  
3 request from the client to communicate with the server, the communication  
4 facilitation mechanism is configured to:

5           produce a session key to be used in communications between the client  
6 and server;

7           create a ticket to the server by encrypting an identifier for the client and  
8 the session key with the temporary secret key for the server;

9           assemble a message that includes the identifier for the server, the session  
10 key and the ticket to the server;

11           send the message to the client in a secure manner; and to

12           allow the client to forward the ticket to the server in order to initiate  
13 communications between the client and the server.

1           39. (Original) The apparatus of claim 38, further comprising a mechanism  
2 within the server that is configured to:  
3           decrypt the ticket received from the client using the temporary secret key  
4 to restore the session key and the identifier for the client; and to  
5           use the session key to protect subsequent communications between the  
6 server and the client.

1           40. (Original) The apparatus of claim 38, wherein the communication  
2 facilitation mechanism is configured to include an expiration time for the session  
3 key in the message.

1           41. (Original) The apparatus of claim 38, wherein the client is configured  
2 to additionally forward an identifier for the temporary secret key to the server, so  
3 that the server can know which temporary secret key to use in decrypting the  
4 ticket.

1           42. (Original) The apparatus of claim 38, wherein in sending the message  
2 to the client in the secure manner, the communication facilitation mechanism is  
3 configured to encrypt the message with a second session key that was previously  
4 communicated to the client by the KDC.

1           43. (Original) The apparatus of claim 38, wherein the communication  
2 facilitation mechanism is configured to alternatively create the ticket to the server  
3 by encrypting the identifier for the client and the session key with one of:  
4           a public key for the server; and  
5           a secret key for the server previously agreed upon between the server and  
6 the KDC and stored at the KDC.

1           44. (Original) The computer-readable storage medium of claim 37, further  
2 comprising an authentication mechanism that is configured to authenticate the  
3 server.

1           45. (Original) The apparatus of claim 44, wherein in authenticating the  
2 server, the authentication mechanism is configured to use authentication  
3 information pertaining to the server, the authentication information including a  
4 certificate chain from a trust anchor to the server, and including a server public  
5 key that is associated with a server private key to form a public key-private key  
6 pair associated with the server.

1           46. (Original) The apparatus of claim 44, wherein in authenticating the  
2 server the authentication mechanism is configured to operate without having prior  
3 configuration information pertaining to the server at the KDC.

1           47. (Original) The apparatus of claim 44, wherein in authenticating the  
2 server, the authentication mechanism is configured to use a server public key that  
3 is stored locally in the KDC.

1           48 (Canceled).

1           49. (Original) The apparatus of claim 37, wherein the communication is  
2 signed with a server private key so that the KDC can use a corresponding server  
3 public key to verify that the communication was sent by the server.

1           50. (Original) The apparatus of claim 37, further comprising a requesting  
2 mechanism within the KDC that is configured to send a request to the server  
3 indicating that the temporary secret key is needed from the server.

1           51. (Original) The apparatus of claim 37, further comprising a sending  
2 mechanism that is configured to send information to the server that enables the  
3 server to authenticate the KDC.

1           52. (Original) The apparatus of claim 37, wherein the KDC is configured  
2 to operate in accordance with the Kerberos standard.

1           53. (Original) The apparatus of claim 37, wherein the communication  
2 received from the server additionally includes an identifier for the server.

1           54. (Original) The apparatus of claim 37, wherein the storage mechanism  
2 is additionally configured to communicate the temporary secret key to multiple  
3 KDCs.

1           55. (New) The method of claim 1, wherein the temporary secret key is  
2 encrypted with a public key belonging to the KDC, so that the temporary secret  
3 key can only be decrypted using a private key belonging to the KDC.

1           56. (New) The computer-readable storage medium of claim 19, wherein  
2 the temporary secret key is encrypted with a public key belonging to the KDC, so  
3 that the temporary secret key can only be decrypted using a private key belonging  
4 to the KDC.

1           57. (New) The apparatus of claim 37, wherein the temporary secret key is  
2 encrypted with a public key belonging to the KDC, so that the temporary secret  
3 key can only be decrypted using a private key belonging to the KDC.